UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/006,465	12/06/2001	Bahman Qawami	M-9913-1 US	3583

36257 7590 02/28/2006

PARSONS HSUE & DE RUNTZ LLP
595 MARKET STREET
SUITE 1900
SAN FRANCISCO, CA 94105

EXAMINER	
GELAGAY, SHEWAYE	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 02/28/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/006,465	QAWAMI ET AL.	
	Examiner	Art Unit	
	Shewaye Gelagay	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 November 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *8-12* is/are allowed.

6)☒ Claim(s) *1,3,5-7 and 13-39* is/are rejected.

7)☐ Claim(s) *2 and 4* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *11/8/05,10/25/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to Applicant's amendment filed on November 3, 2005. Claims 9, 10 and 35 have been amended. Claims 1-39 are pending.

Oath/Declaration

2. The Examiner withdraws the objection to the oath/declaration

Specification

3. The Examiner withdraws the objection to the specification.

Claim Rejections - 35 USC § 112

4. The Examiner withdraws the rejection of claims 5, 12, 22 and 24 under 35 U.S.C. 112.

Claim Rejections - 35 USC § 101

5. The Examiner withdraws the rejection of claims 1-7 and 13-39 under 35 U.S.C. 101.

Response to Arguments

6. Applicant's arguments with respect to claims 1-39 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and

> the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1, 3, 5-7 and 13-14, and 16-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hirota et al. (hereinafter Hirota) U.S. Patent 6,856,431 in view of Tagawa et al. (hereinafter Tagawa) U.S Patent 6,615,192.

As per claim 1:

Hirota teaches a method of accessing an encrypted track on a removable media with a device, the track comprising frames having content, the method comprising:

authorizing the media; (Col. 3, lines 64-67; Col. 57, lines 24-31)

decrypting the track by a process comprising:

(a) calculating a media unique key; (Col. 10, lines 26-29; Col. 57, lines 63-65; Col. 59, lines 3-18) and thereafter

(b) decrypting a title key stored in the memory of the device with the media unique key; (Col. 10, lines 24-25; Col. 59, lines 65-66; Col. 60, lines 5-6) and thereafter

(c) decrypting a group of frames; (Col. 42, lines 34-35; Col. 60, lines 10-11)

(f) repeating (a) through (e) until the entire track is completed. (Col. 47, lines 25-27; Col. 60, lines 11)

In addition, Hirota further discloses when the playback of audio objects which create audio tracks ends, the following audio object is read and when the playback of the following audio object commences, the corresponding management information is read and overwritten into the internal memory of the playback device to take the place of management information that was hitherto stored. (Col. 5, lines 34-39; Col. 20, lines 52-61)

Hirota does not explicitly disclose deleting the decrypted title key; and deleting the media unique key.

Tagawa in analogous art, however, discloses the title and disc key may be deleted whenever copying is performed. (Col. 8, 56-61; Col. 11, lines 32-33)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Hirota to include deleting the decrypted title key and deleting the media unique key. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Hirota (Col. 4, 17-19) in order to minimize the damage caused by the exposure of one of the encryption keys.

As per claim 3:

The combination of Hirota and Tagawa teaches all the subject matter as discussed above. In addition, Tagawa further discloses

decrypting a doubly encrypted title key stored in the media with a session key calculated while authorizing the media to produce a singly encrypted title key; (Col. 59, lines 65-67; and

copying the singly encrypted title key from the media into a memory of the device. (Col. 60, lines 4-6)

As per claims 5 and 14:

The combination of Hirota and Tagawa teaches all the subject matter as discussed above. In addition, Hirota further discloses a method wherein the group of

frames comprises less than one to about five seconds of content in a decoded or decompressed form. (Col. 15, line 51)

As per claim 6:

The combination of Hirota and Tagawa teaches all the subject matter as discussed above. In addition, Hirota further discloses a method wherein decrypting the track comprises decrypting one or more files, the files comprising the frames. Col. 42, lines 34-35; Col. 60, lines 10-11)

As per claim 7:

The combination of Hirota and Tagawa teaches all the subject matter as discussed above. In addition, Hirota further discloses a method comprising decoding and decompressing the track. (Col. 42, lines 34-40)

As per claim 13:

Hirota teaches a system for enabling a device to read an encrypted file having encrypted content from a media, and to write an encrypted file having encrypted content to a media, the system comprising:

a computing unit, and a system memory; (Figure 52, items 3, 4 and 10)

interface means for receiving commands from the device; (Figure 52, item 1)

secure dynamic decryption means configured to:

(a) copy an encrypted title key from the media to a memory of the device, (Col. 12, lines 16-61; Col. 46, lines 10-11)

(b) decrypt the encrypted title key, (Col. 10, lines 24-25; the FileKey used for encrypting the written data is itself encrypted; Col. 59, lines 65-66; Col. 60, lines 5-6; FileKey is decrypted using the master key)

(c) decrypt a portion of encrypted content with the decrypted title key, (Col. 42, lines 34-35; descrambler for decrypting frames using different FileKey for each file; Col. 60, lines 10-11; AOB is decrypted using the encryption key FileKey)

(e) repeat a-d such until all of the content of the file has been decrypted, and wherein the decrypted title keys reside in and are accessible only to the secure means of the system. (Col. 47, lines 25-27; Col. 60, lines 11; music is simultaneously played)

In addition, Hirota further discloses when the playback of audio objects which create audio tracks ends, the following audio object is read and when the playback of the following audio object commences, the corresponding management information is read and overwritten into the internal memory of the playback device to take the place of management information that was hitherto stored. (Col. 5, lines 34-39; Col. 20, lines 52-61)

Hirota does not explicitly disclose delete the decrypted title key. Tagawa in analogous art, however, discloses the title and disc key may be deleted whenever copying is performed. (Col. 8, 56-61; Col. 11, lines 32-33)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Hirota to include deleting the decrypted title key and deleting the media unique key. This modification would have been obvious because a person having ordinary skill in the art would have

been motivated to do so, as suggested by, Hirota (Col. 4, 17-19) in order to minimize the damage caused by the exposure of one of the encryption keys.

As per claim 16:

The combination of Hirota and Tagawa teaches all the subject matter as discussed above. In addition, Hirota further discloses a system wherein the interface means and secure dynamic decryption means are stored in a system memory of the device. (Col. 42, lines 29-42)

As per claim 17:

Tagawa and Dolan teach all the subject matter as discussed above. In addition, Tagawa further discloses a system wherein the interface means and secure dynamic decryption means are executed by the computing unit. (Col. 42, lines 34-56)

9. Claims 15 and 18-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hirota et al. (hereinafter Hirota) U.S. Patent 6,856,431 in view of Tagawa et al. (hereinafter Tagawa) U.S Patent 6,615,192 and further in view of Lau et al. (hereinafter Lau) United States Letter Patent Number 5,790,423.

As per claim 15:

The combination of Hirota and Tagawa teaches all the subject matter as discussed above. Both references do not explicitly disclose a system comprising a digital signal processor.

Lau in analogous art, however, discloses a system comprising a digital signal processor.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Hirota and Tagawa to include a system comprising a digital signal processor. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so in order not to provide a real-time digital signal processing.

As per claim 18:

The combination of Hirota, Tagawa and Lau teaches all the subject matter as discussed above. In addition, Lau teaches a secure dynamic decryption means is stored in memory of the digital signal processor, and executed by the digital signal processor. (Col. 7, lines 4-18)

As per claim 19:

The combination of Hirota, Tagawa and Lau teaches all the subject matter as discussed above. In addition, Lau further discloses a system wherein the interface means is executed by the digital signal processor. (Col. 2, lines 50-Col. 3, line 13)

10. Claims 20-27, 28, and 38-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hirota et al. (hereinafter Hirota) U.S. Patent 6,856,431 in view of Tagawa et al. (hereinafter Tagawa) U.S Patent 6,615,192 and in view of Saxena et al. (hereinafter Saxena) U.S. Patent 5,805,821.

As per claim 20:

Hirota teaches a system that enables a device to decrypt a file having encrypted content on a secure medium, the system comprising:

one or more user interface modules for receiving commands from the device; (Figure 52, item 1)

a security engine for decrypting the encrypted content and the one or more encrypted keys sent from the secure medium to a memory of the device, the decrypted keys used to decrypt the encrypted content, (Col. 42, lines 34-40) wherein

the one or more keys are contained in an encrypted data segment, and the security engine (a) decrypts one or more of the keys, (Col. 10, lines 24-25; Col. 59, lines 65-66; Col. 60, lines 5-6) (b) decrypts a portion of the encrypted content using the one or more decrypted keys, (Col. 42, lines 34-35; Col. 60, lines 10-11) and (d) repeats (a)-(c) until all portions of the content are decrypted. (Col. 47, lines 25-27; Col. 60, lines 11)

In addition, Hirota further discloses the playback apparatus includes a card connector for connecting the playback apparatus to the flash memory card. (Col. 42, lines 27-28) and when the playback of audio objects which create audio tracks ends, the following audio object is read and when the playback of the following audio object commences, the corresponding management information is read and overwritten into the internal memory of the playback device to take the place of management information that was hitherto stored. (Col. 5, lines 34-39; Col. 20, lines 52-61)

Hirota does not explicitly disclose an applications programming interface for receiving the commands from the one or more user interface modules and managing the retrieval and storage of encrypted content from the secure medium; and delete the decrypted title key. Tagawa in analogous art, however, discloses the title and disc key may be deleted whenever copying is performed. (Col. 8, 56-61; Col. 11, lines 32-33)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Hirota to include deleting the decrypted title key and deleting the media unique key. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Hirota (Col. 4, 17-19) in order to minimize the damage caused by the exposure of one of the encryption keys.

Both references do not explicitly disclose an applications programming interface for receiving the commands from the one or more user interface modules and managing the retrieval and storage of encrypted content from the secure medium. Saxena in analogous art, however, discloses an applications programming interface for receiving the commands from the one or more user interface modules and managing the retrieval and storage of encrypted content from the secure medium. (Col. 18, lines 34-43)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Hirota and Tagawa to include an applications programming interface for receiving the commands from the one or more user interface modules and managing the retrieval and storage of encrypted content from the secure medium. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Saxena (Abstract) in order to provide a capability for specifying commands for execution by the user interface and in response to the command for controlling at least on storage device using a synchronous application program interface.

As per claim 21:

The combination of Hirota, Tagawa and Saxena teaches all the subject matter as discussed above. In addition, Hirota further discloses a system wherein the content is encoded in the AAC, MP3 or WMA format. (Col. 56, lin14-18)

As per claim 22:

The combination of Hirota, Tagawa and Saxena teaches all the subject matter as discussed above. In addition, Hirota further discloses a system wherein the one or more keys are in a decrypted state for the time it takes to decrypt and process less than one second to about five seconds of decoded content. (Col. 5, lines 34-39; Col. 20, lines 52-61; Col. 15, line 51)

As per claim 23:

The combination of Hirota, Tagawa and Saxena teaches all the subject matter as discussed above. In addition, Hirota further discloses a system wherein the data segment comprising the one or more encrypted keys is buffered and decrypted in fractional portions. (Col. 58, lines 20-32)

As per claim 24:

The combination of Hirota, Tagawa and Saxena teaches all the subject matter as discussed above. In addition, Hirota further discloses a system wherein the fractional portion is about 512 bytes. (Col. 57, line 61)

As per claim 25:

The combination of Hirota, Tagawa and Saxena teaches all the subject matter as discussed above. In addition, Hirota further discloses a system wherein the device comprises a computing unit, system memory, and a hardware interface. (Figure 52)

As per claim 27:

The combination of Hirota and Tagawa teaches all the subject matter as discussed above. In addition, Hirota further discloses a system wherein the interface means and secure dynamic decryption means are stored in a system memory of the device. (Col. 42, lines 29-42)

As per claim 28:

The combination of Hirota and Tagawa teaches all the subject matter as discussed above. In addition, Hirota further discloses wherein the interface means and secure dynamic decryption means are executed by the computing unit. (Col. 42, lines 34-56)

As per claims 38 and 39:

The combination of Hirota and Tagawa teaches all the subject matter as discussed above. In addition, Hirota further discloses wherein the security engine further comprises a random number generator, the generator utilizing two or more system timers to create the random number. (Col. 57, lines 13-23)

11. Claims 26, 29-32 are rejected under 35 U.S.C. 103(a) as being unpatentable Hirota et al. (hereinafter Hirota) U.S. Patent 6,856,431 in view of Tagawa et al. (hereinafter Tagawa) U.S Patent 6,615,192 and in view of Saxena et al. (hereinafter

Saxena) U.S. Patent 5,805,821 and further in view of Lau et al. (hereinafter Lau) United States Letter Patent Number 5,790,423.

As per claim 26:

The combination of Hirota, Tagawa and Saxena teaches all the subject matter as discussed above. Both references do not explicitly disclose a system comprising a digital signal processor.

Lau in analogous art, however, discloses a system comprising a digital signal processor.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Hirota, Tagawa and Saxena to include a system comprising a digital signal processor. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so in order not to provide a real-time digital signal processing.

As per claim 31:

The combination of Hirota, Tagawa, Saxena and Lau teaches all the subject matter as discussed above. In addition, Lau teaches a secure dynamic decryption means is stored in memory of the digital signal processor, and executed by the digital signal processor. (Col. 7, lines 4-18)

As per claim 29-30 and 32:

The combination of Hirota, Tagawa, Saxena and Lau teaches all the subject matter as discussed above. In addition, Lau further discloses a system wherein the

interface means is executed by the digital signal processor. (Col. 2, lines 50-Col. 3, line 13)

12. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hirota et al. (hereinafter Hirota) U.S. Patent 6,856,431 in view of Tagawa et al. (hereinafter Tagawa) U.S Patent 6,615,192 and further in view of Ansell et al. (hereinafter Ansell) United States Letter Patent Number 6,367,019.

As per claim 3:

The combination of Hirota and Tagawa teaches all the subject matter as discussed above. Both references do not explicitly disclose decrypting a doubly encrypted title key stored in the media with a session key calculated while authorizing the media to produce a singly encrypted title key.

Ansell in analogous art, however, discloses decrypting a doubly encrypted title key stored in the media with a session key calculated while authorizing the media to produce a singly encrypted title key. (Col. 7, line 19)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Tagawa and Dolan to include decrypting a doubly encrypted title key stored in the media with a session key calculated while authorizing the media to produce a singly encrypted title key. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Ansell (Col. 7, lines 20-22) in order not to have a secure communication between the media and the device.

13. Claims 33-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hirota et al. (hereinafter Hirota) U.S. Patent 6,856,431 in view of Tagawa et al. (hereinafter Tagawa) U.S Patent 6,615,192 and in view of Saxena et al. (hereinafter Saxena) U.S. Patent 5,805,821 and further in view of Turgeon United States Publication Number 2003/0014371.

As per claim 33:

The combination of Hirota, Tagawa and Saxena teaches all the subject matter as discussed above. Both references do not explicitly disclose a non-secure interface(s) for accessing the unencrypted content of the medium.

Turgeon in analogous art, however, discloses a non-secure interface(s) for accessing the unencrypted content of the medium. (Page 1, paragraph 12)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Hirota, Tagawa and Saxena to include a non-secure interface(s) for accessing the unencrypted content of the medium. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so in order to make the system versatile by allowing access to demos and samples.

As per claim 34:

The combination of Hirota, Tagawa, Saxena and Turgeon teaches all the subject matter as discussed above. In addition, Hirota further discloses a system comprising a security manager module. (Col. 9, line 66-Col. 10, line 2)

As per claim 35:

The combination of Hirota, Tagawa, Saxena and Turgeon teaches all the subject matter as discussed above. In addition, Hirota further discloses a system wherein the secure interface(s) communicate with the security manager module and module communicates with the security engine. (Col. 58, line 54-Col. 60, line 13)

As per claim 36:

The combination of Hirota, Tagawa, Saxena and Turgeon teaches all the subject matter as discussed above. In addition, Hirota further discloses a system comprising a device driver, the security engine accessing the content and keys through the device driver. (Col. 10, lines 15-30)

As per claim 37:

The combination of Hirota, Tagawa, Saxena and Turgeon teaches all the subject matter as discussed above. In addition, Turgeon further discloses a system wherein each of the one or more engines for processing and transmitting audio, video or images further comprising a non-secure application programming for accessing unencrypted content of the medium. (Page 1, paragraph 12)

Allowable Subject Matter

14. Claims 8-12 are allowed.

15. The following is an examiner's statement of reasons for allowance.

16. Independent claim 8 is directed to a method of accessing an encrypted data file on a removable media with a dive. None of the prior art either taken alone or in combination teach or suggest method of accessing an encrypted data file on a

removable media with a device, the data file comprising frames having content, the method comprising:

authorizing the media for a user session by a process comprising:

calculating a media key; and thereafter

calculating a media unique key from the media key; and thereafter

deleting the media key; and thereafter

calculating a session key from the media unique key; and thereafter

deleting the media unique key.

decrypting a doubly encrypted title key stored in the media with the session key to produce a singly encrypted title key;

copying the singly encrypted title key from the media into a memory of the device; and

decrypting the file by a process comprising:

(a) calculating the media unique key; and thereaRer

(b) decrypting the title key stored in the memory of the device with the media unique key; and thereafter

(c) decrypting a group of frames; and thereafter

(d) deleting the decrypted title key;

(e) deleting the media unique key;

(f) repeating (a) through (e) until the entire file is completed.

Therefore, the claims are allowable over the cited prior art.

17. Claim 2 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. Claim 2 is allowed because it has similar limitations as claim 8.

Claim 4, which is directly or indirectly dependents of claim 2 is also objected.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shewaye Gelagay
2/20/06

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER